

109TH CONGRESS
1ST SESSION

H. R. 1099

To criminalize Internet scams involving fraudulently obtaining personal information, commonly known as phishing.

IN THE HOUSE OF REPRESENTATIVES

MARCH 3, 2005

Ms. HOOLEY (for herself, Mr. ENGEL, and Mr. CASE) introduced the following bill; which was referred to the Committee on the Judiciary

A BILL

To criminalize Internet scams involving fraudulently obtaining personal information, commonly known as phishing.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Anti-phishing Act of
5 2005”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

8 (1) American society is increasingly dependent
9 on the Internet for communications, entertainment,
10 commerce, and banking.

1 (2) For the Internet to reach its full potential
2 in these and other respects, it must continue to be
3 a trustworthy medium. This means, for example,
4 that Internet users should be able to trust the stated
5 origin of Internet communications and the stated
6 destination of Internet hyperlinks.

7 (3) Internet users are increasingly subjected to
8 scams based on misleading or false communications
9 that trick the user into sending money, or trick the
10 user into revealing enough information to enable
11 various forms of identify theft that result in finan-
12 cial loss.

13 (4) One class of such scams, called “phishing”,
14 uses false e-mail return addresses, stolen graphics,
15 stylistic imitation, misleading or disguised
16 hyperlinks, so-called “social engineering”, and other
17 artifices to trick users into revealing personally iden-
18 tifiable information. After obtaining this informa-
19 tion, the “phisher” then uses the information to cre-
20 ate unlawful identification documents and/or to un-
21 lawfully obtain money or property.

22 (5) These crimes victimize not only the individ-
23 uals whose information is stolen, but the entire on-
24 line community, including millions of people who rely

1 on the integrity of the Internet’s system of addresses
2 and hyperlinks.

3 **SEC. 3. CRIMINAL OFFENSE.**

4 (a) IN GENERAL.—Chapter 63 of title 18, United
5 States Code, is amended by adding at the end the fol-
6 lowing:

7 **“§ 1351. Internet fraud**

8 “(a) WEBSITE.—Whoever knowingly, with the intent
9 to carry on any activity which would be a Federal or State
10 crime of fraud or identity theft—

11 “(1) creates or procures the creation of a
12 website or domain name that represents itself as a
13 legitimate online business, without the authority or
14 approval of the registered owner of the actual
15 website or domain name of the legitimate online
16 business; and

17 “(2) uses that website or domain name to in-
18 duce, request, ask, or solicit any person to transmit,
19 submit, or provide any means of identification to an-
20 other;

21 shall be fined under this title or imprisoned up to five
22 years, or both.

23 “(b) MESSENGER.—Whoever knowingly, with the in-
24 tent to carry on any activity which would be a Federal
25 or State crime of fraud or identity theft—

1 “(1) falsely represents itself as being sent by a
2 legitimate online business;

3 “(2) includes an Internet information location
4 tool that refers or links users to an online location
5 on the World Wide Web that falsely purports to be-
6 long to or be associated with such legitimate online
7 business; and

8 “(3) induces, requests, asks, or solicits a recipi-
9 ent of the electronic mail message directly or indi-
10 rectly to provide, submit, or relate any means of
11 identification to another;

12 shall be fined under this title or imprisoned up to five
13 years, or both.

14 “(c) DEFINITIONS.—In this section:

15 “(1) The term ‘domain name’ has the meaning
16 given that term in section 46 of the Act entitled ‘An
17 Act to provide for the registration and protection of
18 trade-marks used in commerce, to carry out the pro-
19 visions of certain international conventions, and for
20 other purposes’ (in this subsection referred to as the
21 ‘Trademark Act of 1946’) (15 U.S.C. 1127).

22 “(2) The term ‘Internet’ has the meaning given
23 that term in section 230(f)(1) of the Communica-
24 tions Act of 1934 (47 U.S.C. 230(f)(1)).

1 “(3) The term ‘electronic mail message’ has the
2 meaning given that term in section 3 of the CAN–
3 SPAM Act of 2003 (15 U.S.C. 7702).

4 “(4) The term ‘initiate’ has the meaning given
5 that term in section 3 of the CAN–SPAM Act of
6 2003 (15 U.S.C. 7702).

7 “(5) The term ‘procure’ means intentionally to
8 pay or provide consideration to, or induce, another
9 person to create a website or domain name.

10 “(6) The term ‘recipient’ has the meaning given
11 that term in section 3 of the CAN–SPAM Act of
12 2003 (15 U.S.C. 7702).

13 “(7) The term ‘Internet information location
14 tool’ when used in this section has the meaning
15 given that term in section 231 of the Communica-
16 tions Act of 1934 (47 U.S.C. 231).

17 “(8) The term ‘means of identification’ when
18 used in this section has the meaning given that term
19 in section 1028 of this title.”.

20 (b) CHAPTER ANALYSIS.—The chapter analysis for
21 chapter 63 of title 18, United States Code, is amended
22 by adding at the end the following:

“1351. Internet fraud.”.

○

1 (2) For the Internet to reach its full potential
2 in these and other respects, it must continue to be
3 a trustworthy medium. This means, for example,
4 that Internet users should be able to trust the stated
5 origin of Internet communications and the stated
6 destination of Internet hyperlinks.

7 (3) Internet users are increasingly subjected to
8 scams based on misleading or false communications
9 that trick the user into sending money, or trick the
10 user into revealing enough information to enable
11 various forms of identity theft that result in finan-
12 cial loss.

13 (4) One class of such scams, called “phishing”,
14 uses false e-mail return addresses, stolen graphics,
15 stylistic imitation, misleading or disguised
16 hyperlinks, so-called “social engineering”, and other
17 artifices to trick users into revealing personally iden-
18 tifiable information. After obtaining this informa-
19 tion, the “phisher” then uses the information to cre-
20 ate unlawful identification documents and/or to un-
21 lawfully obtain money or property.

22 (5) These crimes victimize not only the individ-
23 uals whose information is stolen, but the entire on-
24 line community, including millions of people who rely